ТАХОГРАФИЧЕСКИЙ КОНТРОЛЬ
ПРАВИЛА ОРГАНИЗАЦИИ РАБОТЫ ПВК И МАСТЕРСКИХ

Версия 1.0

Листов 23

Санкт-Петербург
2022 г.

Содержание

1 ВВЕДЕНИЕ

1.1 Термины и сокращения

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
АРМП	АРМ подготовки данных, обеспечивающее взаимодействие с УЦ в процессе активизации НКМ
Заявитель	Физическое лицо или представитель Юридического лица, Индивидуального предпринимателя, действующий по доверенности – Заявитель на выпуск КТ, КСЭП, активизацию НКМ и КСЭП или представитель заявителя, чей сертификат будет использоваться в КТ или НКМ
ИЗКТ	Информационная система персональных данных «Интерфейс заказов КТ» (кратное наименование ИС ПДн ИЗКТ)
ИС	Информационная система
КСЭП	Ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи
КТ	Карта тахографа
КЭП	Квалифицированная электронная подпись
Мастерская	Организация, занимающаяся активизаций НКМ, в том числе, оформлением заявлений на КСЭП и записью КСЭП в НКМ
НКМ	Навигационно-криптографический модуль (блок СКЗИ тахографа)
НСД	Несанкционированный доступ
ОИ	Организация-изготовитель карт тахографа
Оператор ПВД	Оператор первичного ввода данных
Оператор ПДн	Организация, которая занимается обработкой персональных данных
ПВК	Пункт выдачи карт – организация, занимающаяся оформленем заявлений на карты тахографа и выдачей карт тахографа, в том числе, заявлений на КСЭП и выдачу КСЭП
ПДн	Персональные данные
ПЭП	Простая электронная подпись
СЗИ	Средства защиты информации
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр, выпускающий КСЭП для использования в картах тахографов и НКМ
ЦТО	Центр технического обслуживания

1.2 Участники бизнес-процессов

1.2.1 Регулятор

Министерство транспорта Российской Федерации

1.2.2 Организации-изготовители карт тахографа

1) АО «НТЦ «СПЕЦПРОЕКТ» (с 2018г.)
2) ООО «ИКЦ Транспортные технологии» (с 2019г.)
3) ООО «Инвента» (с 2019г.)
4) ООО «Лэда-СЛ» (с 2020г.)
5) ООО «КМ211» (с 2020г.)

1.2.3 Удостоверяющий центр

Аккредитованный Удостоверяющий Центр

1.2.4 Оператор ИС ПДн ИЗКТ

ООО «Современные технологии снабжения» (с 2013 г.)

1.3 Нормативно-правовые акты

Приказ Минтранса России от 28.10.2020 N 440 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства» https://legalacts.ru/doc/prikaz-mintransa-rossii-ot-28102020-n-440-ob-utverzhdenii/

Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» https://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-01112012-n-1119

Приказ ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» https://legalacts.ru/doc/prikaz-fapsi-ot-13062001-n-152-ob/

Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» https://legalacts.ru/doc/ukaz-prezidenta- rf-ot-06031997-n-188/

Приказ ФСТЭК России от 18.02.2013 N 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» https://legalacts.ru/doc/prikaz-fstek-rossii-ot-18022013-n-21/

2 ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ К ПВК И МАСТЕРСКИМ

2.1 Требования к ПВК

Организации, осуществляющие приём документов на выпуск КСЭП и КТ, а также выдачу КТ с записанными на них КСЭП для выполнения работ должны:

- **Соответствовать требованиям к Операторам ПДн** (п.3.1).
- **Иметь лицензию на работу с СКЗИ** с соответствующими разрешёнными видами деятельности (только в случае осуществления выдачи КТ) (п.3.2).
- **Быть действующим доверенным лицом УЦ** (п.3.3).
- **Иметь действующий агентский договор с ОИ** (п.3.4).
- **Иметь действующий договор на право использования ЭВМ «ИЗКТ» и «СКЗИ» на условиях простой лицензии** для организации информационного обмена с УЦ и ОИ, а также подключение к ИС ПДн ИЗКТ через защищённую сеть (п.3.6).

2.2 Требования к Мастерским

Для выполнения работ по активизации блоков СКЗИ тахографа организация должна:

- **Соответствовать требованиям к Операторам ПДн** (п.3.1).
- **Иметь лицензию на работу с СКЗИ** с соответствующими разрешёнными видами деятельности (п.3.2).
- **Быть действующим доверенным лицом УЦ** (п.3.3).
- **Иметь действующий агентский договор**, по крайней мере, с одним **ЦТО** (п.3.5).
- **Быть учтена в перечне сведений о мастерских**, осуществляющих деятельность по установке, проверке, техническому обслуживанию и ремонту тахографов.
- **Иметь действующие карты тахографов (мастерской).**
- **Иметь действующую лицензию на АРМ активизации** для организации информационного обмена с УЦ и ЦТО, а также подключение к соответствующим серверам через защищённую сеть.

3 ТРЕБОВАНИЯ ПО ВИДАМ ДЕЯТЕЛЬНОСТИ

Представленные в данном разделе требования разработаны с учётом состава и объёма данных, используемых в процессе заказа и выдачи карт тахографа, а также активизации НКМ. В случае если организация или индивидуальный предприниматель осуществляют ещё какой-то вид деятельности, то представленные требования могут потребовать доработки.

3.1 Требования к Оператору ПДн

3.1.1 Организационные требования

- По факту начала деятельности подать уведомление в Роскомнадзор о том, что организация является оператором ПДн (п.4.1).
- Создать орган криптографической защиты (п.4.1.4).
- Организовать режим обеспечения безопасности помещений, в которых размещены АРМ с доступом к ИЗКТ.
- Организовать хранение оригиналов документов в бумажном виде и носителей информации, содержащих ПДн (п.4.1.3).
- Обеспечить сохранность и хранение носителей ПДн.
- Определить перечень лиц, допущенных к ПДн.
- Назначить ответственного за обеспечение безопасности ПДн.
- Создать структурное подразделение или возложить на уже имеющееся структурное подразделение ответственность за своевременное обеспечение соответствия АРМ требованиям по защите информации.
- Организовать контроль доступа к техническим средствам, на которых выполняется обработка ПДн.
- Внедрить организационно-нормативные документы[1] (п.4.1.2).

3.1.2 Технические требования

Требования к рабочему месту Оператора ПДн:

- Использование лицензионной операционной системы, поддерживаемой производителем. Необходимо регулярно проверять наличие обновлений безопасности, выпускаемых производителем операционной системы и своевременно их выполнять.
- Использование только сертифицированного ФСТЭК средства СЗИ для информационных систем с 3-м уровнем защищённости ПДн[2].
- Должно быть установлено лицензионное средство антивирусной защиты, сертифицированное ФСТЭК[3]. Необходимо регулярно выполнять обновления антивирусных баз.

[1] Организационные документы в Приложении №1 представлены как образцы, которые Оператор ПДн может использовать в качестве шаблона для своей организации. Оператор ПДн должен подготовить папку со всеми организационными документами, в которой все документы должны быть заверены и подписаны соответствующими лицами.

[2] Например, Dallas lock 8.0-K SecretNet Studio

3 Например, Касперский, dr-Web

– Для передачи данных между АРМ и сервером ИС должно использоваться сертифицированное СКЗИ С-Терра, совместимое с криптографическим сервером, используемым оператором применяемой ИС.

3.2 Требования по обращению СКЗИ

3.2.1 Разрешённые виды деятельности

Далее указаны необходимые виды деятельности согласно перечню выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

3.2.1.1 Для выдачи КТ

21. Передача и хранение шифровальных (криптографических) средств.

3.2.1.2 Для активизации НКМ

12. Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств.

20. Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

21. Передача шифровальных (криптографических) средств.

3.2.1.3 Организационные требования

Орган криптографической защиты ведёт:

– Поэкземплярный учёт СКЗИ, эксплуатационной и технической документации к ним.
– Контроль за соблюдением правил пользования, хранения СКЗИ и условий их использования.
– Ведение на каждого пользователя СКЗИ лицевого счёта (реестра СКЗИ, эксплуатационной и технической документации к нему, ключевые документы).

Требования к хранению СКЗИ

Помещения, в которых хранятся СКЗИ, должны находиться в пределах контролируемой зоны, иметь прочные двери с замками, гарантирующими надежное закрытие.

Помещения, в которых хранятся СКЗИ, должны находиться под охраной в нерабочее время.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должно быть предусмотрено металлическое хранилище, оборудованное внутренними замками с двумя экземплярами ключей и (или) кодовыми замками, или приспособлениями для опечатывания замочных скважин.

Требования к передаче СКЗИ

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учёта.

Пользователи СКЗИ хранят носители и ключевые файлы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

СКЗИ и ключевые документы могут доставляться специально выделенными нарочными из числа сотрудников органа криптографической защиты или пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

С целью передачи СКЗИ в другие города и регионы необходимо принять следующие меры:

1. Сотрудник, который будет осуществлять передачу СКЗИ, должен иметь доверенность от юридического лица на право передачи СКЗИ.
2. Передача СКЗИ от юридического лица сотруднику, осуществляющему дальнейшую передачу СКЗИ, производится по акту приёма-передачи.
3. Сотрудник, получив СКЗИ, оформляет сопроводительные письма или акты приёма-передачи на имя конечных пользователей.
4. Полученные СКЗИ помещаются в опечатываемый чемодан, исключающий бесконтрольный доступ к СКЗИ и уничтожение СКЗИ.
5. Передача СКЗИ производится в орган криптографической защиты организации или лично пользователю СКЗИ по акту приёма-передачи или сопроводительному письму.
6. В случае если СКЗИ не могут быть переданы в течение рабочего дня, они подлежат возврату юридическому лицу.
   В случае если возврат юридическому лицу невозможен, сотрудник, осуществляющий передачу, должен обеспечить физическую сохранность СКЗИ. Наиболее оптимальным решением будет аренда банковской ячейки, т.к. при данном решении будут соблюдаться требования по наличию сигнализации, прочных дверей, защиты окон и т.п. Одновременно с этим СКЗИ будут находиться в металлическом сейфе.
   Вторым возможным вариантом является аренда помещения и оборудования, подходящих под требования.
7. После передачи СКЗИ сотрудник возвращает в орган криптографической защиты юридического лица подписанные акты приёма-передачи или сопроводительные письма, по которым орган криптографической защиты осуществляет списание СКЗИ в соответствующих журналах.

Требования к уничтожению СКЗИ

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной

ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

СКЗИ уничтожают (утилизируют) по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с лицензиатом ФСБ России.

Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, в которых они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они становятся (оказываются) полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надёжно удалена (стерта).

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников органа криптографической защиты. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учёта.

Требования по возврату СКЗИ

Возврат СКЗИ производится по акту, с соответствующей записью органом криптографической защиты в журнале поэкремплярного учёта и списанием их с лицевых счетов.

3.3 Требования к доверенному лицу УЦ

3.3.1 Организационные требования

Все сотрудники доверенного лица, формирующие документы в адрес УЦ, должны иметь персональную усиленную квалифицированную электронную подпись.

3.3.2 Технические требования

Для обмена информацией с УЦ доверенное лицо должно быть подключено к ИЗКТ или АРМП, в зависимости от выполняемых функций.

3.4 Требования к агенту ОИ

3.4.1 Организационные требования

Агент ОИ должен:

- Иметь все лицензии, специальные разрешения и иные документы, необходимые для осуществления действий, предусмотренных Договором, в соответствии с требованиями законодательства РФ;
- Иметь на законных основаниях программно-аппаратные средства, а также права использования программ для ЭВМ, необходимые для осуществления действий, предусмотренных Договором;
- Не находиться в состоянии ликвидации либо в процессе банкротства, и его деятельность не должна быть приостановлена в порядке, предусмотренном законодательством Российской Федерации;
- Выполнять требования законодательства РФ по защите персональных данных, подлежащих обработке в связи с исполнением Договора.

3.4.2 Технические требования

Для автоматизации обмена информацией с ОИ агент должен быть подключен к ИЗКТ.

3.5 Требования к агенту ЦТО

Требования к агенту ЦТО:

- Иметь все лицензии, специальные разрешения и иные документы, необходимые для осуществления действий, предусмотренных Договором, в соответствии с требованиями законодательства РФ;
- Иметь на законных основаниях программно-аппаратные средства, а также права использования программ для ЭВМ, необходимые для осуществления действий, предусмотренных Договором;
- Не находиться в состоянии ликвидации либо в процессе банкротства, и его деятельность не должна быть приостановлена в порядке, предусмотренном законодательством Российской Федерации;
- Выполнять требования законодательства РФ по защите персональных данных, подлежащих обработке в связи с исполнением Договора.

3.6 Требования к лицензиату ИС ПДн ИЗКТ

3.6.1 Организационные требования

Лицензиат ИС ПДн ИЗКТ должен:

- Предоставить информацию о реквизитах организации, а также адреса и

GPS-координаты офисов по приёму Заявителей.

- В случае изменения реквизитов организации или данных сотрудников, владельцев учётных записей, в 10-дневный срок внести соответствующие изменения в административном интерфейсе ИЗКТ.
- Создавать учётные записи в ИЗКТ и допускать к работе в ИЗКТ исключительно своих сотрудников.
- Передавать логин и пароль для доступа в ИЗКТ лично в руки сотрудникам, требовать от сотрудников соблюдения конфиденциальности пароля.
- Информировать сотрудников о правилах обработки ПДн.
- Признавать электронным документом всю информацию, подписанную ПЭП сотрудника при работе в ИЗКТ, равнозначным документу на бумажном носителе, подписанному собственноручной подписью в том числе, признавать авторство электронных заявок, подписанных ПЭП сотрудников Лицензиата.

3.6.2 Технические требования

Выполнять требования по защите персональных данных, определённые в разделе «Технические требования» для Оператора ПДн (п.3.1.2).

4 НОРМАТИВНАЯ РЕГУЛЯТОРИКА

4.1 Требования к Оператору ПДн

Согласно ст. 3. Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», Оператором ПДн является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

В случае обработки и передачи персональных данных оператор обязан подать уведомление в Роскомнадзор, как оператор ПДн (Ст. 22. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»).

4.1.1 Защита конфиденциальной информации

Персональные данные в соответствии с Указом Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» являются конфиденциальными сведениями, и их защита осуществляется в соответствии с требованиями защиты конфиденциальной информации.

Оператор ПДн обязан обеспечить техническую защиту обрабатываемых ПДн и, в соответствии с установленным уровнем защищённости (классом защиты), провести оценку эффективности принятых мер (ФЗ от 27.07.2006 N 152-ФЗ «О персональных данных», Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»).

4.1.2 Организационно-нормативные документы

На основании ФЗ от 27.07.06 № 152-ФЗ «О персональных данных» Оператор ПДн должен внедрить следующие организационно-нормативные документы:

- Положения по обеспечению информационной безопасности персональных данных при их обработке.
- Политику в отношении обработки персональных данных.
- Регламент реагирования на запросы субъектов персональных данных.
- Приказ о назначении ответственного за организацию обработки персональных данных.
- Модель угроз безопасности (дублируется в ПП №1119).
- Журнал учёта машинных носителей информации.
- Регламент проведения контрольных мероприятий.
- План внутренних мероприятий.

- Журнал учёта внутренних проверок.
- Порядок уничтожения ПДн и акт об уничтожении ПДн.
- Перечень нормативных документов о защите ПДн.

Организационные документы в Приложении №1 представлены как образцы, которые Оператор ПДн может использовать в качестве шаблона для своей организации. Оператор ПДн должен подготовить папку со всеми организационными документами, в которой все документы должны быть заверены и подписаны соответствующими лицами.

4.1.3 Хранение и уничтожение ПДн

Согласно ФЗ от 27.07.06 № 152-ФЗ «О персональных данных» хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, но не ранее чем через две недели.

Уничтожение ПДн производится в соответствии с порядком об уничтожении ПДн и завершается составлением соответствующего акта.

4.1.4 Работа со средствами криптографической защиты информации (СКЗИ)

Карта тахографа и навигационный криптографический модуль (НКМ) являются средствами криптографической защиты информации (СКЗИ).

Согласно Постановлению Правительства №313 от 16.04.2012г (ред. от 21.12.2020) «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств,….» (с изм. и доп., вступ. в силу с 01.01.2021) Оператор ПДн обязан иметь лицензии ФСБ России на деятельность, связанную со СКЗИ.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации **Оператор ПДн обязан создать орган криптографической защиты** (п. 6 Приказ ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»).

Функции органа криптографической защиты могут быть возложены на физическое лицо.

5 ВЫПУСК КАРТ ТАХОГРАФА СО СКЗИ И АКТИВАЦИЯ НКМ

5.1 Общие сведения

В соответствии с Приказом Министерства транспорта РФ от 28.10.2020 № 440 «Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства» в карту тахографа и блок НКМ должен быть записан квалифицированный сертификат ключа проверки электронной подписи, Федерального закона № 63-ФЗ от 06.04.2011г. «Об электронной подписи».

Заявление на изготовление КСЭП.

При оформлении заявки на изготовление карты тахографа Оператору ПВД необходимо объяснить Заявителю, что он должен подписать Заявление на создание и выдачу ключей электронной подписи, а также создание и выдачу квалифицированного сертификата ключа проверки электронной подписи, который записывается на карту тахографа.

При активизации блока НКМ Заявителю необходимо направить в адрес УЦ Заявление на создание и выдачу ключей электронной подписи, а также на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи.

Расписка в получении КСЭП и уведомление на Госуслугах.

После получения карты Оператору ПВД необходимо объяснить Заявителю, что он должен подписать Расписку в получении ключей электронной подписи и квалифицированного сертификата ключа проверки электронной подписи. После этого Аккредитованный Удостоверяющий центр зарегистрирует данный сертификат в ЕСИА, и Заявителю придёт уведомление на Госуслугах.

Хранение документов.

ПВК обязан хранить Заявление и Расписку на КЭП в течение срока равного сроку действия КТ (карта водителя - 3 года, карта мастерской - 1 год, карта контроллера - 2года, карта предприятия - 3года).

ПВК должен обеспечить безопасное хранение и защиту конфиденциальной информации в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (п.4.1.3).

5.2 Выпуск карт тахографа со СКЗИ

В разделе представлен поэтапный порядок работы Оператора ПВД с Заявителем по выпуску карты тахографа с использованием ИС ПДн ИЗКТ.

5.2.1 Подготовительный этап

Оператор ПВД должен проконсультировать Заявителя по списку документов, которые необходимо предъявить для оформления карты тахографа, а также договориться о времени и месте личной явки Заявителя или его представителя для оформления КТ.

5.2.2 Создание электронной заявки в ИС ПДн ИЗКТ

Оператор ПВД может оформить электронную заявку на изготовление КТ и КСЭП только после проведения идентификации личности по предъявленному документу, удостоверяющему личность Заявителя или представителя Заявителя, при условии его личной явки.

Перед оформлением заявки в ИС ПДн ИЗКТ Оператор ПВД должен предоставить Заявителю следующий список документов для ознакомления:

- Договор оферты между ОИ и Заявителем.
- Правила пользования «Программно-аппаратными шифровальными (криптографические) средствами защиты информации «Карта тахографа «Диамант-2» (ИПФШ.467444.006ПП).

Оператор ПВД обязан убедиться в том, что Заявитель ознакомился с вышеперечисленными документами и взять об этом расписку.

Оператор ПВД должен заверить копии документов (согласно требованиям ОИ), загрузить копии к электронной заявке и сформировать заявления на изготовление КТ и КСЭП.

Заявитель должен лично подписать заявления на изготовление КТ и КСЭП.

Оператор ПВД должен подписать заявление на КСЭП своей персональной усиленной квалифицированной ЭП.

5.2.3 Выдача расписки и квитанции

Оператор ПВД должен распечатать для Заявителя расписку в получении документов, а также квитанцию для оплаты через банк или QR-код через личный кабинет в публичной части ИС ПДн ИЗКТ.

Для подтверждения факта подачи заявления Заявитель должен сказать Оператору ПВД код подтверждения, который придёт ему в смс-сообщении.

Оператор должен ввести код подтверждения в ИС ПДн ИЗКТ, после чего электронная заявка станет доступна для оплаты.

Заявка на изготовление КТ и КСЭП будет передана в работу после зачисления средств на расчётный счёт УЦ и ОИ.

В течение 5 (пяти) рабочих дней принимается положительное или отрицательное решение УЦ об изготовлении КСЭП, а ОИ об изготовлении КТ.

5.2.4 Выдача КТ и КСЭП

Выдача КТ возможна только при личной идентификации Заявителя Оператором ПВД.

Заявитель должен будет подписать документы о получении КСЭП и КТ, об ознакомлении с Правилами пользования и содержимым КСЭП.

Оператор ПВД должен заверить расписку в получении Заявителем КСЭП своей персональной усиленной квалифицированной ЭП.

Заявитель также получает бухгалтерские документы и акт выполненных работ.

В случае неполучения Заявителем КТ в течение заданного времени, ПВК должен отправить КТ обратно в ОИ.

5.3 Активизация блока НКМ

Активизация блока НКМ – это внесение в блок СКЗИ тахографа с использованием карты мастерской установочных данных, включая идентификационные данные транспортного средства и квалифицированные сертификаты ключей проверки электронной подписи блока СКЗИ тахографа.

Для удобства Заявителей процесс занесения данных о Заявителе и транспортном средстве и процесс активизации НКМ разнесены на два рабочих места:

1. АРМП – АРМ подготовки данных для активизации НКМ, обеспечивающее ввод и проверку данных, подготовку документов.
2. АРМА – АРМ мастера активизации СКЗИ тахографа, обеспечивающее взаимодействие с СКЗИ тахографа через карту мастерской.

В разделе представлен поэтапный порядок работы Оператора ПВД с Заявителем на активизацию блока НКМ с использованием ИС ПДн ИЗКТ.

5.3.1 АРМП - Подготовительный этап

На данном этапе личная явка Заявителя не требуется.

Оператор ПВД мастерской создаёт в АРМП электронную заявку, в которую вносит данные о Заявителе и транспортном средстве с оригиналов или электронных образов документов.

После внесения и проверки всех данных заявка на активизацию переводится в статус «Данные готовы к отправке», после этого данные автоматически будут направленны в ведомства для проверки.

Проверка может занимать от нескольких минут до 5 (пяти) рабочих дней. Результат проверки будет отображён в АРМП.

В случае выявления ошибки требуется откорректировать данные, при необходимости, запросить уточнения у Заявителя. Если данные соответствуют документам, то Заявитель должен обратиться в ведомство, выдавшее отказ, для корректировки данных в ведомственной системе.

При успешном прохождении проверки можно планировать проведение активизации блока СКЗИ тахографа.

5.3.2 АРМП – Заявление КСЭП

На этом этапе требуется личная явка Заявителя, а также наличие транспортного средства с установленным тахографом и блоком СКЗИ тахографа.

После успешной проверки и подтверждения ведомствами сведений из заявки можно приступить к процедуре активизации НКМ. Для этого Оператор ПВД мастерской должен:

- Провести личную идентификацию Заявителя в соответствии с требованиями УЦ.
- Распечатать в АРМП заявление на выпуск квалифицированного сертификата ключа проверки электронной подписи и получить личную подпись Заявителя на Заявлении.
- Отсканировать подписанное заявление и загрузить скан в АРМП.

После загрузки заявления данные об активизации автоматически передаются в АРМА, а скан заявления в УЦ.

5.3.3 АРМА – Подготовка запроса на КСЭП, отправка запроса в УЦ

На данном этапе личная явка Заявителя не требуется. Требуется наличие транспортного средства с установленным тахографом и блоком СКЗИ тахографа.

С помощь АРМА, карты мастерской и тахографа с установленным блоком СКЗИ выполняется набор технических операций по формированию запроса на сертификат с данными установленного СКЗИ.

После успешного формирования сертификата в АРМА данные автоматически передаются в АРМП.

5.3.4 АРМП - Расписка КСЭП

На этом этапе требуется личная явка Заявителя, а также наличие транспортного средства с установленным тахографом и блоком СКЗИ тахографа.

После успешного формирования сертификата у Оператора ПВД мастерской появляется возможность распечатать расписку для получения сертификата в АРМП. Для этого Оператор ПВД мастерской должен:

- Провести личную идентификацию Заявителя в соответствии с требованиями УЦ.
- Распечатать в АРМП расписку в получении квалифицированного сертификата ключа проверки электронной подписи, получить личную подпись Заявителя на расписке.
- Отсканировать расписку и загрузить скан в АРМП.

После загрузки расписки данные автоматически передаются в АРМА, а скан расписки в УЦ.

5.3.5 АРМА – Активизация блока НКМ

На данном этапе личная явка Заявителя не требуется. Требуется наличие транспортного средства с установленным тахографом и блоком СКЗИ тахографа.

С помощь АРМА, карты мастерской и тахографа с установленным блоком СКЗИ выполняется набор технических операций по загрузке сертификата в установленный в тахограф блок СКЗИ.

6 ВЫПУСК КАРТ ТАХОГРАФА СО СКЗИ И АКТИВИЗАЦИЯ НКМ НА «ВЫЕЗДЕ»

6.1 Общие сведения

Лицензирование осуществляется в соответствии с Федеральным законом РФ от 04.05.2011 г. N99-ФЗ «О лицензировании отдельных видов деятельности».

Порядок лицензирования деятельности с СКЗИ определен Постановлением Правительства РФ от 16.04.2012 г. N 313, которое было дополнено Постановлением Правительства РФ от 21.12.2020 N 2198 следующим пунктом:

«9.1 Выполнение работ и оказание услуг, указанных в пунктах 12 - 15, 17, 18 и 20 - 24 перечня, не по адресу места осуществления лицензируемой деятельности, указанному в лицензии, не требуют переоформления лицензии.»

Постановлением Правительства РФ от 21.12.2020 N 2198, вступило в силу 01 января 2021 года.

Разъяснения ФСБ по вопросам осуществления деятельности (пункты 12, 20,21) представлены по ссылке – http://clsz.fsb.ru/clsz/license/addons/prilozhenie_N_4.htm

Активизация блока СКЗИ тахографа на «выезде» регламентируется следующими положениями:

- Лицензии ФСБ России действительны и позволяют выполнять работы на всей территории Российской Федерации.
- Объекты, предназначенные для осуществления лицензируемой деятельности или используемые при её осуществлении и соответствующие требованиям п. 8. ст. 3 Федерального закона «О лицензировании отдельных видов деятельности» должны быть внесены в раздел лицензии «Место осуществления лицензируемого вида деятельности» и соответствовать этой записи.
- Отдельные работы (оказываемые услуги), составляющие лицензируемый вид деятельности (определенные пунктами Перечня 12,20,21) могут осуществляться по месту расположения объектов, в отношении которых они выполняются.
- Работы по активизации блока СКЗИ тахографа и самого тахографа должны проводиться только с использованием принадлежащей лицензиату ФСБ России карты тахографа (мастерской).

Для приёма заявления и выдачи КТ на «выезде» необходимо подготовить:

- Ноутбук с «С-Терра клиент» с активным подключением к сети Интернет.
- Портативный принтер/сканер.

Для активизации блока НКМ на «выезде» необходимо подготовить:

- Ноутбук с «С-Терра клиент» с активным подключением к сети Интернет.
- Портативный принтер/сканер.
- Считыватель карт тахографа.
- Карту тахографа (мастреской).

7 ОТВЕТСТВЕННОСТЬ ПВК И МАСТЕРСКИХ

7.1 Ответственность оператора ПДн

Оператор ПДн несёт ответственность согласно КоАП РФ Статья 13.11: Нарушение законодательства Российской Федерации в области персональных данных (в ред. Федерального закона от 07.02.2017 N 13-ФЗ).

Согласно статье 13.11 предусмотрены штрафы от 1000 до 200 000 рублей в зависимости от степени нарушения.

Сотрудник Оператора ПДн несёт личную ответственность за внесение изменений в документы Заявителя, в том числе за подделку подписи в таких документах, согласно УК РФ Статья 327: Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков.

7.2 Ответственность лицензиата ИС ПДн ИЗКТ

Лицензиат ИС ПДн ИЗКТ не имеет права передавать права использования ИС СПДн ИЗКТ (программ для ЭВМ «ИЗКТ 2.0») третьим лицам или предоставлять учётные записи лицам, не являющимся сотрудниками Лицензиата.

При нарушении Лицензиатом требований, которые повлекли или могли бы повлечь за собой нарушение прав Лицензиара, Лицензиар вправе ограничить доступ к ИС ПДн ИЗКТ и взыскать с Лицензиата штраф в размере 1 000 000 (одного миллиона) рублей. При этом убытки возмещаются в полном размере сверх суммы штрафа.

7.3 Ответственность доверенного лица УЦ

В случае нарушения правил и требований УЦ доверенное лицо может быть лишено своего статуса - может быть исключено из реестра доверенных лиц УЦ. В этом случае доверенное лицо УЦ будет лишено возможности информационного взаимодействия с УЦ через ИС ПДн ИЗКТ.

В случае, если в результате деятельности доверенного лица УЦ возникают издержки у УЦ, то такие издержки могут быть переложены на доверенное лицо, в результате деятельности которого они возникли.

Доверенное лицо УЦ несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей. (в ред. Федеральных законов от 30.12.2015 N 445-ФЗ, от 27.12.2019 N 476-ФЗ).

Гражданско-правовая ответственность заключается в том, что доверенное лицо УЦ возмещает вред, причиненный третьим лицам за неисполнение обязанностей, предусмотренных законом и договором, – ст. 15, гл. 59 ГК РФ. Так, если УЦ нарушит регламент и выдаст квалифицированный сертификат ключа проверки электронной подписи не владельцу, а неустановленному лицу, то в случае причинения ущерба владельцу убытки также могут быть взысканы с доверенноголица УЦ.

Федеральным законом от 28.12.2016 № 471-ФЗ была введена ст. 13.33 в Ко-АП http://www.consultant.ru/document/cons_doc_LAW_34661/442dd45f58cf7d213f1e723690e3a0222608ea1e/, которая устанавливает административную ответственность за нарушение обязанностей, предусмотренных законодательством в области электронной подписи.

Размеры административного штрафа варьируются в статье от 10 до 500 тыс. руб. и зависят от степени возможного причинения вреда.

Нарушение доверенным лицом УЦ порядка выдачи квалифицированного сертификата ключа проверки электронной подписи - влечёт наложение административного штрафа на юридическое лицо в размере от 10 до 30 тыс. руб.

За выдачу квалификационного сертификата, содержащего заведомо недостоверную информацию о его владельце, – штраф от 200 до 250 тыс. руб.

За повторные нарушения штрафы взимаются в двукратном размере.

ПРИЛОЖЕНИЕ №1

Ниже представлен полный список нормативно-организационных документов на информационную систему персональных данных, которые Оператор ПДн может использовать как шаблон для своей организации.

Образцы этих документов представлены по ссылке
http://sts.taho-kart.ru/?page_id=474

На основании ФЗ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

- Приказ о назначении ответственного за организацию обработки персональных данных.
- План мероприятий по обеспечению безопасности ПДн.
- Положение об обработке ПДн.
- Перечень персональных данных.
- Политика в отношении обработки персональных данных.
- Регламент реагирования на запросы субъектов персональных данных.
- Инструкция пользователя информационной системы ПДн.
- Инструкция администратора системы защиты ПДн.
- Положение по обеспечению информационной безопасности персональных данных при их обработке.
- Журнал учёта машинных носителей информации.
- Регламент проведения контрольных мероприятий.
- Журнал учёта внутренних проверок.

На основании Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119:

- Приказ о создании комиссии по категорированию и классификации.
- Акт определения уровня защищённости.
- Модель угроз безопасности (конфиденциальный документ).
- Акт установки границ контролируемой зоны (конфиденциальный документ).
- В зависимости от уровня защищённости, оператор:
  - организует режим обеспечения безопасности помещений, в которых размещена информационная система (перечень помещений хранения и обработки);
  - обеспечивает сохранность носителей персональных данных;
  - определяет перечень лиц, допущенных к ПДн (приказ или распоряжение);

- назначает ответственного за обеспечение безопасности персональных данных в информационной системе (приказ или распоряжение);
- определяет перечень лиц, допущенных к содержанию электронного журнала сообщений (приказ или распоряжение);
- организует автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;
- создаёт структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности (приказ или распоряжение).

На основании приказа ФСТЭК России от 18 февраля 2013 г. N 21:

- Инструкция по антивирусной защите.
- Инструкция по работе с средствами защиты информации от несанкционированного доступа (допускается использовать от производителя).
- Разрешительная система доступа (конфиденциальный документ).
- Технический паспорт информационной системы (конфиденциальный документ).
- Проводится оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных

На основании приказа ФАПСИ от 13 июня 2001 г. N 152:

- Приказ о создании органа криптографической защиты или возложение обязанностей.
- Журнал учёта пользователей СКЗИ.
- Журнал поэкземплярного учёта СКЗИ.
- Журнал приёма выдачи СКЗИ.
- Журнал приёма выдачи носителей ключевой информации.